COVINGTON

EU's Highest Court Hears Case on the Validity of the EU Standard Contractual Clauses

July 17, 2019

Data Privacy and Cybersecurity

On July 9, 2019, the European Court of Justice ("ECJ") heard oral argument in <u>Case C-311/18</u>, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems ("Schrems II").

The primary question before the ECJ is whether the European Commission's standard contractual clauses ("SCCs") are valid for transfers of personal data to the United States. Given the widespread reliance on the SCCs for data transfers to the United States and other countries around the world, the ECJ's judgment is likely to have significant ramifications for many organizations.

Covington represents BSA I The Software Alliance² in *Schrems II* and in a separate challenge to the EU-U.S. Privacy Shield now pending before the EU General Court, <u>Case T-738/16</u>, *La Quadrature du Net and Others v Commission* ("*LQDN*").

Background

The case arises from a complaint filed by privacy activist Maximilian Schrems with the Irish Data Protection Commissioner ("DPC") in December 2015. In his complaint, Mr Schrems challenged Facebook Ireland Ltd's transfer of his personal data to Facebook Inc. in the United States under the 2010 controller-to-processor SCCs, set out in Commission Decision 2010/87/EU (the "SCC Decision"). Among other arguments, Mr Schrems pointed to what he described as the situation of "mass surveillance" in the United States, and asserted that EU data subjects do not have adequate judicial remedies under U.S. law where their data is targeted by U.S. authorities. Mr.

¹ The SCCs are European Commission-approved contract terms that an EU-based data exporter enters into with a non-EU based data importer. The clauses impose contractual obligations on both the exporter and the importer to protect transferred data, and also provide rights to the individuals whose personal data is transferred. Once agreed, the SCCs enable an exporter to lawfully transfer personal data from the Union (subject to compliance with other provisions of the EU's General Data Protection Regulation 2016/679 ("GDPR")).

² BSA is a global trade association that represents leading software innovators. More information about BSA is available <u>here</u>.

Schrems asked the DPC to exercise its powers under Article 4(1) of the SCC Decision to block Facebook Ireland's transfer of his personal data to the United States.

After reviewing both the SCC Decision and certain elements of the U.S. national security regime, the DPC issued a Draft Decision. The DPC broadly agreed that U.S. law was deficient, and that the SCCs did not remedy these deficiencies. Conscious that she lacked authority to strike down the SCC Decision, however, the DPC instead asked the Irish High Court to refer the matter to the ECJ for a ruling on the SCC Decision's validity.³

The Irish High Court reviewed the matter and, following oral argument, agreed that it merited a reference to the ECJ. On April 12, 2018, the Irish High Court asked 11 specific questions (available here) of the ECJ.

The parties in the Irish High Court proceedings included the DPC, Facebook Ireland, and Mr. Schrems, as well as BSA I The Software Alliance, the Electronic Privacy Information Center ("EPIC"), Digital Europe, and the U.S. Government. These parties joined the case on referral to the ECJ; in addition, the European Parliament, the European Commission, and several Member States (Austria, Belgium, the Czech Republic, France, Germany, Ireland, the Netherlands, Poland, Portugal and the UK)⁴ also intervened before the ECJ. The ECJ also asked the European Data Protection ("EDPB") to appear at the oral hearing.

The Hearing

Following written pleadings, the ECJ set the case for oral argument before the Grand Chamber, signifying its importance.⁵ The day-long hearing began with statements from the parties and interveners. The judge-rapporteur (Thomas von Danwitz)⁶ and Advocate General ("AG") (Henrik Saugmandsgaard Øe) followed with a number of questions, targeted primarily at the European Commission and EDPB.

The parties and interveners took the following broad positions on the validity of the SCCs:

■ The DPC and EPIC contended that the SCCs do not sufficiently protect EU personal data that has been transferred to the United States; the Austrian Government also expressed skepticism in this regard. The DPC took the view that under the U.S. national security regime, a data subject has no general right to be informed that his or her data

_

³ In striking down the EU-U.S. Safe Harbor in 2014, the ECJ ruled that only the Court -- and not individual data protection authorities -- could invalidate Commission Decisions, see Case C-362/14, *Schrems v Data Protection Commissioner*, para. 52.

⁴ Belgium, the Czech Republic, Poland and Portugal submitted written pleadings, but did not participate in the oral hearing.

⁵ The ECJ sits in a Grand Chamber of 15 Judges for particularly complex or important cases. This is rare, and cases are generally heard by Chambers of three or sometimes five Judges.

⁶ Judge von Danwitz has served as rapporteur in a number of significant ECJ data protection-related decisions, including Case C-362/14, *Schrems v Data Protection Commissioner*, in which the ECJ invalidated the EU-U.S. Safe Harbor.

has been accessed, and no ability to obtain a judicial remedy when it is. The DPC concluded, therefore, that the SCCs should be invalidated for transfers to the United States.

- Mr. Schrems agreed with the DPC and EPIC that the U.S. surveillance regime was insufficiently protective of EU data subjects' rights -- but disagreed with the DPC's conclusion that the SCCs were invalid. Instead, he argued that the DPC should exercise her powers to suspend the transfer of his personal data by Facebook to the United States:
- Facebook, the U.S. Government, the European Commission, the European Data Protection Board, France, Germany, Ireland, the Netherlands, the United Kingdom, and BSA and Digital Europe generally supported the validity of the SCCs.

While participants focused on different issues in their oral statements, arguments touched on several broad themes (many of which were responsive to questions raised by the ECJ in addition to those referred by the Irish High Court):

- The importance of the SCCs to global commerce and communications. Several participants, including Facebook, BSA, Digital Europe, Ireland and the European Commission highlighted the many organizations that rely on the SCCs for global data transfers, and stressed the significant harm their invalidation would have on European businesses and consumers.
- Whether the European Commission was obligated to assess the surveillance practices of a third country before the SCCs could be used to transfer data there. Parties supporting the SCCs' validity argued that EU lawmakers intended the SCCs to be used for transfers to countries that the Commission had not yet deemed "adequate," and therefore that the Commission is not required to review a third country's legal regime before companies may use the SCCs to transfer data there. Instead, these parties argued, the data exporter is responsible both for considering the circumstances of the transfer, including the legal regime in the third country, and for ensuring that the SCCs afford appropriate safeguards for the data being transferred. These parties further argued that it was the job of supervisory authorities to hold exporters accountable for compliance with these obligations.
- The relevance of the EU-U.S. Privacy Shield Decision to the validity of transfers made under the SCCs. Judge von Danwitz in particular was focused on the relationship between the Privacy Shield and the SCCs, and queried (i) how and why Facebook transferred data under both instruments and (ii) whether the DPC could disregard the Commission's findings in the Privacy Shield Decision regarding the adequacy of the U.S. regime. The Commission explained that organizations in practice frequently use both the

__

⁷ Chapter V of the GDPR provides several different mechanisms on which parties can rely to transfer personal data from the EEA. These include "adequacy," where the Commission concludes a third country's legal regime meets EU standards such that data can be transferred there with no further safeguards applied (Article 45, GDPR). Where the Commission has not yet assessed a country as adequate, parties wishing to transfer personal data can rely on the SCCs (among other measures) (Article 46, GDPR).

SCCs and the Privacy Shield. The Commission further explained that the Privacy Shield was not an across-the-board finding that the U.S. legal system was adequate; instead, it affords adequacy only to Privacy Shield-certified organizations that comply with the Shield's requirements. Where data was transferred outside those parameters (i.e. under the SCCs), the Commission argued, the Privacy Shield Decision should not bind supervisory authorities in assessing those transfers. The EDPB broadly agreed.

- Whether the level of protection required under EU law applies both to data that has been transferred and to data in transit. Several parties, including Austria, the European Parliament, the DPC, and EPIC answered this question in the affirmative. Other parties pointed out the complexity of applying such a requirement, given that controllers do not know how data would travel through the internet and given that governments are not transparent about their surveillance practices in relation to data moving through undersea cables.
- U.S. surveillance practices. The U.S. Government provided an in-depth description of the various limits in U.S. law on government surveillance, many of which were adopted in response to concerns from U.S. partners following Edward Snowden's revelations about U.S. surveillance practices in 2016. The U.S. Government also described the layered oversight regime, designed to balance the needs of state security against personal privacy, and extensively discussed use of selectors by U.S. authorities to target data access requests.
- Judicial redress for EU individuals whose personal data is accessed by U.S. authorities. Both the DPC and Mr. Schrems questioned the ability of EU data subjects to obtain judicial redress in the United States. The U.S. Government rebutted the contention that U.S. remedial measures were insufficient. A number of parties also pointed out the various remedies available to data subjects in the EU, where data subjects are more likely to want to avail themselves of such remedies.
- The role of the EU Courts when reviewing the national security practices of third countries. Several parties, including Facebook and a number of Member States, highlighted the unique balance that must be struck when weighing privacy interests against national security, and encouraged the ECJ not to hold third countries to a higher standard than that expected from EU Member States.

Next Steps

As is the norm in ECJ cases, the AG will issue an opinion prior to the ECJ's decision, setting out his views on how the case should be decided. The AG indicated that he will publish his opinion on December 12, 2019. The ECJ's final decision will likely be announced in the first quarter of 2020.

While the outcome of the case remains uncertain, we expect it to have significant implications for those organizations that rely on the SCCs for transfers to the United States and, potentially, other jurisdictions. Given the ECJ's questions, the ECJ's ruling may also impact the pending LQDN challenge to the EU-U.S. Privacy Shield.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our team, all of whom attended the hearing:

<u>Lisa Peets</u>	+44 20 7067 2031	lpeets@cov.com
Kristof Van Quathem	+32 2 549 52 36	kvanquathem@cov.com
Bart Van Vooren	+1 202 662 5566	bvanvooren@cov.com
Sam Choi	+44 20 7067 2054	jchoi@cov.com
Gemma Nash	+44 20 7067 2316	gnash@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.